

19. Analyze the practical applications of Kerberos in securing e-mails and web communications. Discuss its advantages and limitations.
20. Detail the architecture and components of an Intrusion Detection System (IDS). Discuss how it relates to firewall design principles and overall network security.
-

APRIL/MAY 2025

**23UEDA42B — NETWORK SECURITY
(ELECTIVE – IV)**

Time : Three hours

Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL questions.

1. Define network security.
2. List any two differences between security attacks and security services.
3. Define OSI security architecture.
4. What are the basic principles of classical encryption techniques?
5. What is Simple Data Encryption Standard (SDS)?
6. What is a Message Authentication Code (MAC)?
7. State the role of hash functions in network security.
8. What is the purpose of Kerberos in authentication?



9. How can be an Intrusion Detection System be defined?

10. What are the main functions of a firewall?

SECTION B — ($5 \times 5 = 25$ marks)

Answer ALL questions.

11. (a) Explain the design principles of block ciphers.

Or

(b) Discuss the modes of operation of block ciphers.

12. (a) Outline Euclid's algorithm and its use in cryptography.

Or

(b) Discuss the role of number theory in network security.

13. (a) What are the security implications of hash functions?

Or

(b) Compare SHA and HMAC in terms of security.

14. (a) Discuss the X.509 authentication services.

Or

(b) Explain the significance of IP Security (IPSec).

15. (a) What are common types of viruses and their countermeasures?

Or

(b) Describe the principles of trusted systems in network security.

SECTION C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Discuss the different types of security attacks and the services that can be implemented to mitigate them. Provide examples.

17. Derive the key concepts and applications of modular arithmetic in public key cryptography.

18. Describe the process of authentication in detail, focusing on the mechanisms involved in MAC and hash functions. How do they ensure security?

